

**ENCIPHERING SYSTEM, DECIPHERING SYSTEM, INFORMATION
CONCEALMENT PROCESSING SYSTEM AND INFORMATION-CONCEALED
COMMUNICATION SYSTEM**

Patent Number: JP9006232
Publication date: 1997-01-10
Inventor(s): SAKA YASUHIKO
Applicant(s): RICOH ELEMEX CORP.; RICOH CO LTD
Requested Patent: ☐ JP9006232
Application Number: JP19950154513 19950621
Priority Number(s):
IPC Classification: G09C1/00; G06F9/06; H04L9/00; H04L9/10; H04L9/12
EC Classification:
Equivalents:

Abstract

PURPOSE: To provide a system which enables ciphering and deciphering to be carried out with efficiency without a program being falsified.

CONSTITUTION: Enciphered enciphering/deciphering processing programs Pr1, Pr2,... are transmitted from an information processing device to an IC card by an initial program IP when a password agrees, the IC card deciphers these programs with a deciphering key of a rightful user and sends them back. An information processing device disposes these programs in a work memory area PA, causes them to get started and carried out data enciphering/deciphering processing. Accordingly, these programs, being normally in an enciphered condition, are neither analyzed nor falsified by a third party. After the rightful user has completed data processing, the deciphered plain programs are erased so as not to leave room for the plain programs surviving after the processing, and security of these programs is thereby assured. Enciphering work can be carried out with efficiency without a need for work of taking a storage medium of these programs out of a deposit place and setting it in the information processing device.

Data supplied from the esp@cenet database - I2

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-6232

(43) 公開日 平成9年(1997) 1月10日

(51) Int.Cl. ^a	識別記号	庁内整理番号	F I	技術表示箇所
G 0 9 C 1/00		7259-5 J	G 0 9 C 1/00	
G 0 6 F 9/06	5 5 0		G 0 6 F 9/06	5 5 0 A
H 0 4 L 9/00			H 0 4 L 9/00	Z

審査請求 未請求 請求項の数21 O L (全 20 頁)

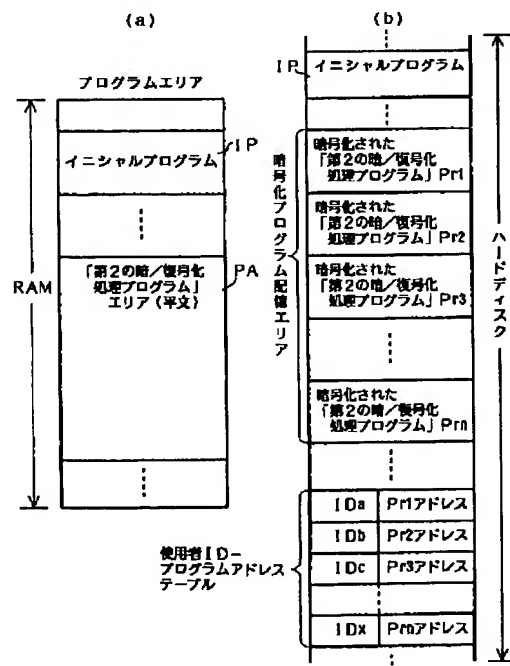
(21) 出願番号	特願平7-154513	(71) 出願人	000006932 リコーエレクトロニクス株式会社 名古屋市中区錦二丁目 2 番13号
(22) 出願日	平成7年(1995) 6月21日	(71) 出願人	000006747 株式会社リコー 東京都大田区中馬込 1 丁目 3 番 6 号
		(72) 発明者	坂 康彦 愛知県名古屋市東区泉 2 丁目28番24号 リ コーエレクトロニクス株式会社内
		(74) 代理人	弁理士 足立 勉

(54) 【発明の名称】 暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システム

(57) 【要約】

【目的】 プログラムが改竄されることなく暗号化・復号化を効率的に行うことができるシステムを提供すること。

【構成】 イニシャルプログラムIPにより、パスワードが合致すると情報処理装置からICカードへ暗号化された暗/復号化処理プログラムPr1, Pr2, ...が送信され、ICカードはこのプログラムを正当使用者の復号化鍵にて復号化し送り返す。情報処理装置はこのプログラムを作業メモリ領域PAに配置して起動しデータの暗/復号化処理を行う。従って通常、プログラムは暗号化されているので第三者により解析されず改竄もできない。正当使用者がデータの処理を完了した後はその平文のプログラムは消去されるため、処理後も平文のプログラムは残っていない、プログラムの安全性が確保される。このため暗号化/復号化処理毎にプログラムの記憶媒体を保管場所から取り出して情報処理装置にセットする作業をしなくても良く効率的に暗号化作業ができる。



【特許請求の範囲】

【請求項1】プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第2暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする暗号化システム。

【請求項2】更に、前記第2暗号化鍵を、第3暗号化鍵にて暗号化する鍵暗号化手段と、前記鍵暗号化手段にて暗号化された前記第2暗号化鍵を、前記暗号化データに付加する鍵付加手段と、を備えた請求項1記載の暗号化システム。

【請求項3】前記鍵付加手段が、前記プログラムの機能として実現されている請求項2記載の暗号化システム。

【請求項4】前記プログラムが、第2暗号化鍵を演算にて求める請求項1～3のいずれかに記載の暗号化システム。

【請求項5】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項1記載の暗号化システム。

【請求項6】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記第3暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請求項3記載の暗号化システム。

【請求項7】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵および前記第3暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項3記載の暗号化システム。

【請求項8】前記付属装置が、前記第3暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項6または7記載の暗号化システム。

【請求項9】前記付属装置が、前記復号化鍵または前記第3暗号化鍵を直接記憶せず、前記復号化鍵または前記第3暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第3暗号化鍵を生成する請求項5～7のいずれかに記載の暗号化システム。

【請求項10】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項1～9記載の暗号化システム。

【請求項11】プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第2復号化鍵にて復号化させて復号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする復号化システム。

【請求項12】更に、前記暗号化データに含まれる暗号化された第2復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項11記載の復号化システム。

【請求項13】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記

プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項1記載の復号化システム。

【請求項14】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項12記載の復号化システム。

【請求項15】本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、

前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、

前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項12記載の復号化システム。

【請求項16】前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項13～15のいずれかに記載の復号化システム。

【請求項17】前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項11～16記載の復号化システム。

【請求項18】請求項1～10のいずれか記載の暗号化システムと請求項11～17記載の復号化システムとが組合わされてなる情報秘匿処理システム。

【請求項19】前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項1～10のいずれか記載の暗号化システム。

【請求項20】前記暗号化データを通信回線を介して受信する受信手段を備える請求項11～17のいずれか記載の復号化システム。

【請求項21】請求項19記載の暗号化システムと請求項20記載の復号化システムとが組合わされてなる情報秘匿通信システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システム、プログラムに基づく復号化処理により暗号化データを復号

化する復号化システム、更にこれらの機能を有する情報秘匿処理システムおよび情報秘匿通信システムに関する。

【0002】

【従来の技術】従来、情報（「データ」とも言う。）内容を秘匿するための手法として、暗号化鍵を用いて秘匿したい情報を暗号化する処理が知られている。情報が一旦暗号化されると、同一の暗号化鍵あるいは特定の復号化鍵を用いないと人間が解読できる状態に戻すことはできないため、そのような暗号化鍵や復号化鍵を有していない他人にとってはその情報の内容を秘密にすることができる。

【0003】しかし、暗号化鍵や復号化鍵（以下、「暗／復号化鍵」として表す。）が漏洩すれば、たちまち他人に情報が解読されてしまうことから、この暗／復号化鍵に対しても、別の暗号化鍵にて暗号化して保管することにより安全性を高めるファイルセキュリティシステムが提案されている（特開平6-102822号公報）。

【0004】

【発明が解決しようとする課題】しかし、このようなシステムにおいても、次のような問題が存在した。すなわち、情報の暗号化処理あるいは情報解読のための復号化処理は、一般的には、コンピュータシステムを用いた情報処理装置にて、暗号化プログラムあるいは復号化プログラム（以下、「暗号化・復号化プログラム」として表す）によりなされるのが普通である。

【0005】この暗号化・復号化プログラムにより、情報が暗号化され、更に安全性を高めるために、その暗／復号化鍵まで暗号化した場合、一見、その情報自体は極めて安全であるように考えられる。ところが、この暗号化・復号化を行う暗号化・復号化プログラム自体は、情報自体よりも無防備であることが多い。もし、この暗号化・復号化プログラムのアルゴリズムが第三者により解析されると、暗号化された情報の解読に利用される恐れがある。

【0006】また、第三者が、その暗号化・復号化プログラム自体を、正当な使用者に解らないように改竄し、第三者が知っている暗号化鍵にて暗号化する機能を付加することにより、その後、暗号化された情報をすべて第三者が解読してしまう恐れもある。更に、暗号化・復号化プログラム内に、暗号化する前の平文状態（暗号化されていない状態を言う。）の情報を第三者が管理する領域にもコピーしてしまう機能を付加する恐れもあった。

【0007】勿論、暗号化・復号化プログラムを使用しない場合には、暗号化・復号化プログラムを厳重に保管することも考えられるが、使用毎に、フロッピー等を保管場所から取り出して、情報処理装置にセットして暗号化・復号化プログラムをロードする処理を行わなくてはならず、暗号化・復号化処理が効率的に行うことができない。

【0008】本発明は、第三者に改竄されることなく、かつ暗号化・復号化を効率的に行うことができる暗号化システム、復号化システム、情報秘匿処理システムおよび情報秘匿通信システムを提供することを目的とする。

【0009】

【課題を解決するための手段】請求項1記載の発明は、プログラムに基づく暗号化処理によりデータを暗号化する暗号化システムにおいて、前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第2暗号化鍵にて暗号化させて暗号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする暗号化システムである。

【0010】請求項2記載の発明は、更に、前記第2暗号化鍵を、第3暗号化鍵にて暗号化する鍵暗号化手段と、前記鍵暗号化手段にて暗号化された前記第2暗号化鍵を、前記暗号化データに付加する鍵付加手段と、を備えた請求項1記載の暗号化システムである。

【0011】請求項3記載の発明は、前記鍵付加手段が、前記プログラムの機能として実現されている請求項2記載の暗号化システムである。請求項4記載の発明は、前記プログラムが、第2暗号化鍵を演算にて求める請求項1～3のいずれかに記載の暗号化システムである。

【0012】請求項5記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項1記載の暗号化システムである。

【0013】請求項6記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記第3暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える請

求項3記載の暗号化システムである。

【0014】請求項7記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵および前記第3暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える請求項3記載の暗号化システムである。

【0015】請求項8記載の発明は、前記付属装置が、前記第3暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶する請求項6または7記載の暗号化システムである。請求項9記載の発明は、前記付属装置が、前記復号化鍵または前記第3暗号化鍵を直接記憶せず、前記復号化鍵または前記第3暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵または前記第3暗号化鍵を生成する請求項5～7のいずれかに記載の暗号化システムである。

【0016】請求項10記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項1～9記載の暗号化システムである。

【0017】請求項11記載の発明は、プログラムに基づく復号化処理により暗号化データを復号化する復号化システムにおいて、前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶するプログラム暗号化記憶手段と、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出すプログラム読出手段と、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化するプログラム復号化手段と、前記プログラム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第2復号化鍵にて復号化させて復号化データとするプログラム起動手段と、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去するプログラム消去手段と、を備えたことを特徴とする復号化システムである。

【0018】請求項12記載の発明は、更に、前記暗号化データに含まれる暗号化された第2復号化鍵を、使用者に対応する復号化鍵にて復号化する鍵復号化手段を備えた請求項11記載の復号化システムである。

【0019】請求項13記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗

号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える請求項1記載の復号化システムである。

【0020】請求項14記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える請求項12記載の復号化システムである。

【0021】請求項15記載の発明は、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とからなり、前記本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、前記付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える請求項12記載の復号化システムである。

【0022】請求項16記載の発明は、前記付属装置が、前記復号化鍵を直接記憶せず、前記復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、前記復号化鍵を生成する請求項13～15のいずれかに記載の復号化システムである。

【0023】請求項17記載の発明は、前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有する請求項11～16記載の復号化システムである。

【0024】請求項18記載の発明は、請求項1～10のいずれかに記載の暗号化システムと請求項11～17記載の復号化システムとが組合わされてなる情報秘匿処理システムである。請求項19記載の発明は、前記暗号化データを通信回線を介して相手方に送信する送信手段を備える請求項1～10のいずれかに記載の暗号化システムである。

【0025】請求項20記載の発明は、前記暗号化データを通信回線を介して受信する受信手段を備える請求項11～17のいずれかに記載の復号化システムである。請求項21記載の発明は、請求項19記載の暗号化システムと請求項20記載の復号化システムとが組合わされてなる情報秘匿通信システムである。

【0026】

【作用及び発明の効果】請求項1の暗号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プロ

グラム復号化手段、プログラム起動手段およびプログラム消去手段を備え、プログラム暗号化記憶手段は、暗号化処理用のプログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶する。プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出す。プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化する。プログラム起動手段は、前記プログラム復号化手段により復号化されたプログラムを起動させることにより、暗号化対象データを第2暗号化鍵にて暗号化させて暗号化データとする。プログラム消去手段は、前記プログラム起動手段にて暗号化対象データの暗号化が完了すると、復号されて起動対象となった前記プログラムを消去する。

【0027】このように、本発明の暗号化システムにて起動する暗号化処理用のプログラムは、暗号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても暗号化処理用のプログラムを復号化することはできない。

【0028】正当な使用者がデータを暗号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化対象データが第2暗号化鍵にて暗号化されて暗号化データとなる。

【0029】しかも、データの暗号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることがなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【0030】上記構成に更に、鍵暗号化手段および鍵付加手段を加えても良い。この鍵暗号化手段は、前記第2暗号化鍵を、第3暗号化鍵にて暗号化する。そして、鍵付加手段は、前記鍵暗号化手段にて暗号化された前記第2暗号化鍵を、前記暗号化データに付加する。

【0031】このように、データを暗号化するための第2暗号化鍵を、更に第3暗号化鍵にて暗号化しているの

で、鍵付加手段にて、暗号化データに第2暗号化鍵を付加しておいても安全は確保できる。また、暗号化データに第2暗号化鍵が付加されるので、その記憶媒体のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、第3暗号化鍵さえ保管されていれば、暗号化データを復号化することができる。すなわち、暗号化データに付加されている暗号化された第2暗号化鍵を第3暗号化鍵にて復号化し、次に復号化された第2暗号化鍵にて、暗号化データを復号化することができる。尚、鍵付加手段は、前記暗号化用のプログラムの機能として実現されていても良い。

【0032】更に、この場合、第2暗号化鍵が、前記暗号化用のプログラムにより演算にて求められたものであっても良い。このように演算にて求められる暗号化鍵は一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時的な鍵も、上記暗号化用のプログラムにて演算されていることから、暗号化処理時以外は、その第2暗号化鍵を生成するプログラムは暗号化されたもののみが存在しているので、第三者が知っている鍵を生成するように改竄することはできない。

【0033】また、本暗号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ICカードとする構成が挙げられる。

【0034】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【0035】このように構成すると、暗号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【0036】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記第3暗号化鍵を記憶するとともに、前記鍵暗号化手段を備える構成としても良い。

【0037】このように構成すると、付属装置側には、第3暗号化鍵と鍵暗号化手段とが存在するため、その第

3暗号化鍵および鍵暗号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵および前記第3暗号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵暗号化手段を備える構成としても良い。

【0038】このように構成すると、付属装置側には、使用者に対応する復号化鍵、第3暗号化鍵、プログラム復号化手段および鍵暗号化手段とが存在するため、その使用者に対応する復号化鍵、第3暗号化鍵、プログラム復号化手段のプログラムおよび鍵暗号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【0039】また、前記付属装置が、第3暗号化鍵を、復号化を許可する者の管理コードと対応したリストとして記憶していても良い。このように構成されていると、管理コード、例えばIDにて復号化を許可する者を指定すれば、付属装置の鍵暗号化手段がそのIDに対応した第3暗号化鍵にて第2暗号化鍵を暗号化することができる。

【0040】また、前記付属装置が、復号化鍵または第3暗号化鍵を直接記憶せず、復号化鍵または第3暗号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵または第3暗号化鍵を生成するものとしても良い。特に、第3暗号化鍵が多数記憶しなくてはならない場合に、演算式のみで良いのでメモリの節約となる。

【0041】また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【0042】請求項11の復号化システムは、プログラム暗号化記憶手段、プログラム読出手段、プログラム復号化手段、プログラム起動手段およびプログラム消去手段とを備え、プログラム暗号化記憶手段は、前記プログラムを、使用者に対応する第1暗号化鍵により暗号化した状態で記憶し、プログラム読出手段は、前記プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段は、前記プログラム読出手段により読み出された前記プログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段は、前記プログラ

ム復号化手段により復号化された前記プログラムを起動させることにより、暗号化データを第2復号化鍵にて復号化させて復号化データとし、プログラム消去手段は、前記プログラム起動手段にて暗号化データの復号化が完了すると、復号化されて起動対象となった前記プログラムを消去する。

【0043】このように、本発明の復号化システムにて起動する復号化処理用のプログラムは、復号化処理に用いられていない場合には、プログラム暗号化記憶手段により暗号化された状態で記憶されている。したがって、暗号化されたままでは、第三者により、解析されることはなく、また解析できないので改竄もできない。また、復号化鍵は使用者が所持することにより、第三者にプログラム復号化手段が判明しても復号化処理用のプログラムを復号化することはできない。

【0044】正当な使用者が暗号化データを復号化する場合には、プログラム読出手段が、プログラム暗号化記憶手段内から、使用者に対応する第1暗号化鍵にて暗号化された前記プログラムを読み出し、プログラム復号化手段が、そのプログラムを、使用者に対応する復号化鍵により復号化し、プログラム起動手段が、その復号化されたプログラムを起動させる。この起動された前記プログラムの機能により、暗号化データを第2復号化鍵にて復号化させて復号化データ、すなわち平文データとすることができる。

【0045】しかも、暗号化データの復号化が完了した後は、プログラム消去手段が、その起動された平文状態のプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出してコンピュータにセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【0046】上記構成に更に、鍵復号化手段を加えても良い。この鍵復号化手段は、暗号化データに含まれる暗号化された第2復号化鍵を、使用者に対応する復号化鍵にて復号化する。このようにすることにより、暗号化データを復号化するための第2復号化鍵が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。

【0047】また、本復号化システムは、本体装置と、この本体装置とは別体に構成され前記本体装置に対して信号的に任意に接続したり切断したりすることが可能な付属装置とに別れて構成されていても良い。例えば、本体装置を、コンピュータ装置とし、付属装置を、ICカードとする構成が挙げられる。

【0048】この場合、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラ

ム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段を備える構成としても良い。

【0049】このように構成すると、復号化処理をしない場合には、本体装置から付属装置を切り離して、安全な保管場所に収納しておくことができる。付属装置側には、使用者に対応する復号化鍵とプログラム復号化手段とが存在するため、その復号化鍵およびプログラム復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。

【0050】また、同様に、本体装置と付属装置とに別々に構成された場合に、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム復号化手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、使用者に対応する復号化鍵を記憶するとともに、前記鍵復号化手段を備える構成としても良い。

【0051】このように構成すると、付属装置側には、使用者に対応する復号化鍵と鍵復号化手段とが存在するため、その復号化鍵および鍵復号化手段のプログラムの安全性が共に確保され、データの安全性が一層確保される。また、本体装置と付属装置とに別々に構成された場合に、上記両者を加味した構成、すなわち、本体装置が、前記プログラム暗号化記憶手段、前記プログラム読出手段、前記プログラム起動手段、および前記プログラム消去手段を備え、付属装置が、前記使用者に対応する復号化鍵を記憶するとともに、前記プログラム復号化手段および前記鍵復号化手段を備える構成としても良い。

【0052】このように構成すると、付属装置側には、使用者に対応する復号化鍵、プログラム復号化手段および鍵復号化手段とが存在するため、その使用者に対応する復号化鍵、プログラム復号化手段のプログラムおよび鍵復号化手段のプログラムの安全性がすべて確保され、データの安全性が一層確保される。

【0053】また、前記付属装置が、復号化鍵を直接記憶せず、復号化鍵が必要とされた場合に、対応する管理コードを用いた演算にて、復号化鍵を生成するものとしても良い。また前記プログラムが、所定時間以内に使用者により次の入力操作が行われない場合に、自己の処理を中止して、前記プログラム消去手段の処理を実行させる機能を有するものとしても良い。このようにすれば、正当な使用者がシステム装置から一旦離れたとしても、しばらくすると平文状態のプログラム自体が消え去るので第三者に解析されたり改竄されたりすることがない。

【0054】また、上述したいずれかの構成の暗号化システムと上述したいずれかの復号化システムとを組合わせて、情報秘匿処理システムとして構成しても良い。このことにより、一つの情報秘匿処理システムにて、暗号化システムと復号化システムとの両方の機能を有するこ

とができ、使用者の処理が効率的となるとともに、プログラムやデータの安全性も確保される。

【0055】尚、上述した暗号化システムにおいて、暗号化データを通信回線を介して相手方に送信する送信手段を備えて、例えば暗号化機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。また、上述した復号化システムにおいても同様に、暗号化データを通信回線を介して受信する受信手段を備えて、例えば暗号化データの解読機能を有するファクシミリ装置等のデータ通信システムとして構成することができる。

【0056】勿論、上述の送信手段を有する暗号化システムと上述の受信手段を有する復号化システムとを組合わせ、暗号化機能および暗号化データ解読機能を有するファクシミリ装置等の情報秘匿通信システムとして構成することができる。

【0057】

【実施例】図1および図2は、本発明の情報秘匿処理システムの一実施例を示している。この内、図1は、情報処理装置2のブロック図を示す。情報処理装置2は、CPU4、ROM6、RAM8、バックアップRAM10、キーボード12、光磁気ディスク(MOD)ドライブ14、CRTディスプレイ16、ハードディスク(HD)装置18、フロッピーディスク(FD)ドライブ20および入出力インターフェイス(I/O)22を備えている。これらの構成はバス24にて信号的に接続され、更にI/O22にはICカードリーダー26が接続されている。

【0058】このように、情報処理装置2はコンピュータとして構成され、ROM6、光磁気ディスクドライブ14に挿入された光磁気ディスク、ハードディスク装置18、フロッピーディスクドライブ20に挿入されたフロッピーディスクあるいはICカードリーダー26に挿入されたICカード30(図2)から読み込まれたプログラムやデータに基づいて、必要な処理を実行し、結果として得られたデータを、光磁気ディスクドライブ14に挿入された光磁気ディスク、ハードディスク装置18、フロッピーディスクドライブ20に挿入されたフロッピーディスクあるいはICカードリーダー26に挿入されたICカード30に記憶する。情報処理装置2は、これ以外にCD-ROMドライブ装置や磁気テープ記憶装置等を備えても良い。

【0059】図2にICカード30のブロック図を示す。ICカード30は、CPU32、ROM34、RAM36、バックアップRAM38および入出力インターフェイス(I/O)40を備えている。これらの構成はバス42にて信号的に接続されている。尚、I/O40は、情報処理装置2のICカードリーダー26に対するコネクタを備えたインターフェイスである。

【0060】前記情報処理装置2の電源オンにより、図

3(a)に示すごとくRAM8のプログラムエリアに、データを暗号化および復号化するためのイニシャルプログラムIPがハードディスク装置18からロードされて起動される。尚、ハードディスク装置18には、図3

(b)に示すごとく、イニシャルプログラムIP以外に、複数の暗号化された「第2の暗/復号化処理プログラム」Pr1~Prnが格納されている。これらの「第2の暗/復号化処理プログラム」Pr1~Prnは、本情報処理装置2の使用者の暗号化鍵(第1暗号化鍵)にて暗号化されたものであり、使用者の数だけ存在し、復号化すれば基本的には同じ機能を有しているプログラムである。ただし、後述するごとく使用者毎に異なる機能を持たせることもできる。使用者とプログラムとの対応は、図3(b)に示すハードディスク装置18内の使用者ID-プログラムアドレステーブルを参照することにより行われる。これらの「第2の暗/復号化処理プログラム」Pr1~Prnおよび使用者ID-プログラムアドレステーブルは、前記イニシャルプログラムIPとともにハードディスク装置18に予めインストールされている。

【0061】また、ICカード30のバックアップRAM38には、図4に示すごとく、パスワード照合プログラムPr11、暗号化処理プログラムPr12、復号化処理プログラムPr13、鍵暗号化処理プログラムPr14および鍵復号化処理プログラムPr15等のプログラムと、正当な使用者のパスワード、正当な使用者のID、正当な使用者の暗/復号化鍵(第1暗号化鍵および復号化鍵に該当する)および正当な使用者がデータの復号化を許可する相手のID(ID1, ID2, ..., IDn)とそのIDに対応する相手方暗号化鍵K1, K2, ..., Knが記憶されている。

【0062】使用者が、データを暗号化するために、情報処理装置2を電源オンした場合には、図5および図6のフローチャートに示すイニシャルプログラムIPが起動される。まず、ステップS100にて初期化処理が行われ、情報処理装置2に存在する各種構成の初期状態を設定し、プログラムに使用するデータの初期値を決定する等の処理がなされる。

【0063】次に、ICカードリーダー26にICカード30が装着されているか否かが判定される(S110)。装着されていないならばステップS110にては否定判定されて、ICカード30の装着を要求する表示をCRTディスプレイ16に行って(S120)、再度ステップS110を実行する処理を繰り返す。

【0064】ICカード30が、ICカードリーダー26に装着されれば、ステップS110にて肯定判定されて、次にパスワードを要求する表示がCRTディスプレイ16になされる(S130)。このパスワードは、図4に示したICカード30の正当な使用者のパスワードを求めるものである。

【0065】パスワードの入力がキーボード12からな

されたか否かが判定され(S140)、入力が無ければ、ステップS150にてタイムアウトと判定されるまで、ステップS140、S150の処理を繰り返す。タイムアウトに該当する所定時間経過してもパスワードの入力がなされなければステップS150にて、肯定判定されて、本イニシャルプログラムの処理を終了する。タイムアウトする前にパスワードの入力があれば、ステップS140にて肯定判定されて、入力されたパスワードがICカード30側へ送信される。そして、次に、ICカード30側からパスワードの照合結果とその使用者のIDとが送信されて来るのを待つ(S170)。

【0066】図7～図8のフローチャートにICカード30側の処理を示す。本処理はICカード30がICカードリーダー26に装着された際に起動される処理である。まず、情報処理装置2からのパスワードの受信待ちとなる(S500)。前述したステップS160の処理により、パスワードが送信されて来ればステップS500にて肯定判定されて、パスワード照合プログラムPr1により、図4に示したバックアップRAM38に記憶された、このICカード30の正当な使用者のパスワードと、情報処理装置2から送られたパスワードとの照合がなされる(S520)。

【0067】そして、その照合の結果と正当な使用者のIDとが情報処理装置2側へ送信される(S530)。次に照合結果が「合致」、すなわち、情報処理装置2からのパスワードとバックアップRAM38内に記憶されていた正当な使用者のパスワードとが一致すれば、正当な使用者がそのICカード30を使用していることが判るので、次にその正当な使用者の暗/復号化鍵を、バックアップRAM38から読み出す(S550)。もし、パスワードの照合結果が不一致となった場合に、ステップS540にて否定判定されて、再度ステップS500の処理に戻る。

【0068】ステップS550を処理した場合には、次に情報処理装置2からの送信待ちとなる(S560)。ステップS530の処理にて、照合結果とIDとが情報処理装置2へ送信されると、情報処理装置2側では、ステップS170にて肯定判定されて、次に合致したか否かが判定される(S180)。合致していなければ、正当な使用者では無いので、ステップS180にて否定判定されて、CRTディスプレイ16に、不一致であることと処理を中止するとの表示をして(S190)、ステップS110の処理に戻る。したがって、ICカード30がICカードリーダー26に装着されていれば、再度、ステップS130にてパスワードが要求され、ステップS140、S150にて、パスワード入力待ちとなる。パスワードの入力を間違えても、再度、入力を求められるので正当な使用者ならば訂正すれば良い。しかし、不正な使用である場合には、パスワードを繰り返して入力させるのは一致の可能性が高くなるので、パスワードの入力間

違いは例えば3回までとし、ステップS180にて3回目の間違いの場合には、ステップS110に戻さず、本イニシャルプログラムを終了するようにする。

【0069】ステップS180にて、合致したとの判定がなされると、CRTディスプレイ16に合致した旨の表示がなされ(S200)、次にICカード30から照合結果と共に受信したIDに対応する暗号化された第2の暗/復号化処理プログラムをハードディスク装置18の記憶ファイルから探し出して、ICカード30側へ送信する(S210)。IDからプログラムを探すのは、図3(b)に示したごとく、ハードディスク装置18にファイルされている使用者ID-プログラムアドレステーブルから、IDに対応する暗号化された第2の暗/復号化処理プログラムのディスク上のアドレスを得て、そのアドレスから該当する暗号化された第2の暗/復号化処理プログラムを読み出すことにより行われる。例えば、使用者のIDがIDbであれば、暗号化された第2の暗/復号化処理プログラムPr2が対応していることが、使用者ID-プログラムアドレステーブルから判明し、そのディスクアドレスから、暗号化された第2の暗/復号化処理プログラムPr2が読み出される。

【0070】次に、ICカード30からの送信待ちとなる(S220)。ICカード30側では、情報処理装置2から暗号化された第2の暗/復号化処理プログラムPr2の送信があると、ステップS560の判定にて肯定判定されて、次にそのプログラムPr2の受信とその受信したプログラムPr2の復号化処理がなされる(S570)。すなわち、バックアップRAM38に存在する復号化処理プログラムPr13を起動して、情報処理装置2から送信されて来たプログラムPr2を復号化する。尚、プログラムPr2が長くて、バッファや作業メモリ容量の関係で一度に送信あるいは復号化できない場合には、分割して送信あるいは復号化しても良い。

【0071】次に、復号化した第2の暗/復号化処理プログラムPr2を情報処理装置2へ送信する(S580)。次に、暗号化していない一時鍵および復号化対象者IDが受信されたか否かが判定され(S590)、受信していなければ、暗号化された一時鍵が受信されたか否かが判定される(S595)。これも受信していなければ、暗号化していない第2の暗/復号化処理プログラムが受信されたか否かが判定される(S600)。いずれも受信していない内は、ステップS590、ステップS595およびステップS600の判定を繰り返す。

【0072】情報処理装置2側では、ICカード30側から、復号化された、すなわち平文の第2の暗/復号化処理プログラムPr2を受信すると、ステップS220にて肯定判定されて、その平文の第2の暗/復号化処理プログラムPr2を、図2(a)に示すごとくRAM8の作業メモリ領域PAに転送する(S230)。

【0073】次に、この平文の第2の暗/復号化処理プ

プログラムPr2がイニシャルプログラムから起動される(S240)。その第2の暗/復号化処理プログラムPr2のフローチャートを図9～図12に示す。この処理がステップS240の起動処理により実行される。

【0074】第2の暗/復号化処理プログラムPr2の処理が開始されると、まず、処理メニューがCRTディスプレイ16に表示される(S1010)。メニューは、暗号化処理(S1100)、復号化処理(S1200)、第2の暗/復号化処理プログラムの変更処理(S1300)およびその他の処理(S1400)である。

【0075】ここで、使用者により暗号化処理(S1100)が選択されると、図10に示す処理が開始される。まず、暗号化対象データ名および復号化対象者IDの入力が要求される(S1102)。暗号化対象データ名は、光磁気ディスクドライブ14にセットされた光磁気ディスク、ハードディスク装置18あるいはフロッピーディスクドライブ20にセットされたフロッピーディスク内のファイルを指定することにより行う。ここでは、光磁気ディスクに暗号化データを格納するため、暗号化対象データは、フロッピーディスクに存在するものとする。

【0076】また復号化対象者IDは、復号化を許可する相手のIDを入力する。復号化を許可する相手方が複数であれば複数のIDを入力する。尚、予め登録されているグループのIDを入力すれば、そのグループに属している複数の相手のIDを指定したことになり、一つのIDで複数人を復号化対象者としてすることができる。

【0077】ここで、タイムアウト処理(S1106)にて所定のタイムアウト時間が経過するまで、入力待ちとなる(S1104)。タイムアウトまで、入力がなければ、ステップS1106にて肯定判定されて、直ちにイニシャルプログラムへ帰るが、暗号化対象データ名および復号化対象者IDの入力がなされれば、次に一時鍵(第2暗号化鍵)を生成する(S1108)。

【0078】ここで、一時鍵の生成は、生成毎に異なる鍵(値や文字列)であることが好ましい。例えば、M系列乱数発生プログラムによる方法やキー操作の時間間隔を10万分の1秒程度で測定して下位の必要桁数のみ取り出す方法等が挙げられる。こうして生成された一時鍵と復号化対象者IDとをICカード30側へ送信し(S1110)、次にICカード30側から送信されて来る暗号化された一時鍵の受信待ちとなる(S1120)。

【0079】ICカード30側では、一時鍵と復号化対象者IDとを受信したので、図8のステップS590にて肯定判定されて、次に、一時鍵暗号化処理プログラムPr14により、復号化対象者IDに対応する相手方暗号化鍵により一時鍵を暗号化する(S610)。ICカード30のバックアップRAM38には、図4に示したごとく、正当な使用者がデータの復号化を許可する相手のID1、ID2、…、IDnとそのIDに対応する相手方

暗号化鍵K1、K2、…、Knが記憶されていることから、例えば、復号化対象者IDがID2であれば、対応する相手方暗号化鍵K2が選択され、その相手方暗号化鍵K2により一時鍵を暗号化する。また、グループのIDが入力されていれば、そのグループの代表となる者のIDから相手方暗号化鍵を選択してその相手方暗号化鍵にて一時鍵を暗号化してもよく、またグループ独自の相手方暗号化鍵にて一時鍵を暗号化しても良い。

【0080】次にこのように暗号化された一時鍵を情報処理装置2側へ送信し(S620)、ICカード30での処理はステップS500の処理に戻る。情報処理装置2側では、暗号化された一時鍵を受信したので、ステップS1120にて肯定判定されて、暗号化された一時鍵を、IDとともに記憶媒体にファイルとして格納する(S1130)。この記憶媒体は、使用者が指定する記憶媒体であるが、ここでは、光磁気ディスクドライブ14にセットされた光磁気ディスクである。勿論、フロッピーディスクあるいはハードディスク装置18その他の記憶媒体でも良い。

【0081】次に既にステップS1102にて入力されている暗号化対象データが読み出され(S1140)、暗号化されていない一時鍵、すなわちステップS1108で生成されたままの一時鍵により、その暗号化対象データが暗号化される(S1150)。このようなデータを鍵を用いて暗号化処理するプログラムとしては、米国の標準アルゴリズムであるDESや、NTT社が開発したFEELE等が知られている。

【0082】次に、この暗号化されたデータを、IDおよび暗号化された一時鍵が格納されたファイルに格納する(S1160)。すなわち、図13に示すごとく、ヘッダ部として、復号者(復号を許可する者)のID(1)、ID(2)、…、ID(n)とそのIDに対応した暗号化一時鍵K(1)、K(2)、…、K(n)とのリストを記載し、データ部として、一時鍵にて暗号化した暗号化データを記載したファイルとして格納する。

【0083】こうして、情報処理装置2にて暗号化処理(S1100)が終了し、次にRAM8上に、例えば、ステップS1140の処理にてRAM8の作業メモリ領域に読み出されたままの暗号化対象データといった、暗号化されていないデータが存在する場合には、そのデータをクリアする処理(S1500)が行われる。

【0084】こうして、第2の暗/復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図6に示すステップS250の処理が行われて、RAM8上に存在している第2の暗/復号化処理プログラムをクリアし、ステップS110の処理に戻る。

【0085】このようにして、データの暗号化が終了する。上述したごとく、本実施例の情報処理装置2にて起動する暗号化処理用のプログラム(図9、図10)は、暗号化処理に用いられていない場合には、ハードディス

ク装置18により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【0086】正当な使用者がデータを暗号化する場合には、ハードディスク装置18から、正当な使用者の暗／復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗／復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化対象データを一時鍵（第2暗号化鍵）にて暗号化させて暗号化データとすることができる。

【0087】しかも、データの暗号化が完了した後は、その起動されたプログラムを消去する。このため、暗号化処理をした後も、平文状態の暗号化用のプログラムが残っていることもなく、暗号化用のプログラムの安全性が確保され、結果として、暗号化されたデータの安全性も確保される。したがって、暗号化処理毎に、暗号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置2にセットしてロードする作業をしなくても良く、効率的に暗号化作業ができる。

【0088】また、暗号化前のデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、一時鍵（第2暗号化鍵）は、相手方暗号化鍵（第3暗号化鍵）にて暗号化される。そして、この暗号化された一時鍵は復号化を許可する者のIDとともに、暗号化データと一つのファイルに収納される。

【0089】このように、データを暗号化するための一時鍵（第2暗号化鍵）を、更に相手方暗号化鍵（第3暗号化鍵）にて暗号化しているので、暗号化データに一時鍵（第2暗号化鍵）を付加しておいても安全は確保できる。また、暗号化データに一時鍵（第2暗号化鍵）が付加されるので、その記憶媒体（ここでは光磁気ディスク）のまま持ち運んだり、あるいはその暗号化データを通信により相手方に送信しても、持ち運び先あるいは通信相手先にて、相手方暗号化鍵（第3暗号化鍵）さえ保管されていれば、暗号化データを復号化することができる。

【0090】一時鍵（第2暗号化鍵）は、前記暗号化用のプログラムにより演算にて求められたものである。このようにデータを暗号化するための暗号化鍵は、その時の暗号化のためだけの一時的な鍵であり、継続して使用されるものではないので、よりデータの安全性が確保される。また、この一時鍵も、前記暗号化用のプログラム内で演算されていることから、暗号化処理時以外は、そのプログラムは暗号化されたもののみが存在しているので、第三者は自分が知っている鍵を生成するように改竄することはできない。

【0091】また、本実施例の情報秘匿処理システムは、本体装置としての情報処理装置2と、この情報処理装置2とは別体に構成され情報処理装置2に対して信号

的に任意に接続したり切断したりすることが可能な付属装置としてのICカード30とに別れて構成され、しかも、情報処理装置2が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の各プログラムを備え、ICカード30が、正当な使用者の暗／復号化鍵および相手方暗号化鍵（第3暗号化鍵）を記憶するとともに、プログラム復号化処理および鍵暗号化処理の各プログラムを備える構成とされている。すなわち、ICカード30側には、正当な使用者の暗／復号化鍵、相手方暗号化鍵（第3暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムが存在するため、その正当な使用者の暗／復号化鍵、相手方暗号化鍵（第3暗号化鍵）、プログラム復号化処理のプログラムおよび鍵暗号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【0092】次に、図13に示した暗号化データファイルを格納した光磁気ディスクを受け取った場合、そのデータを復号化する処理について説明する。使用者は、まず、情報処理装置2の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ14にセットし、自己のICカード30をICカードリーダー26にセットする。

【0093】情報処理装置2では、イニシャルプログラムが起動される。この場合の処理は、ステップS100からステップS240までは、データ暗号化の際に説明した通りである。ICカード30においても同様である。勿論、使用者が異なれば、ICカード30も異なることから、ステップS170にて受信するIDも異なり、ステップS210にてICカード30へ送信される暗号化された第2の暗／復号化処理プログラムも異なる。

【0094】例えば、使用者のIDがIDaであれば、暗号化された第2の暗／復号化処理プログラムPr1が対応していることから、暗号化された第2の暗／復号化処理プログラムPr1が、ICカード30へ送信され、その結果、ステップS240により起動されるプログラムは、第2の暗／復号化処理プログラムPr1が実行される。尚、ここでは、第2の暗／復号化処理プログラムPr1は第2の暗／復号化処理プログラムPr2と同じ内容であるとして説明する。

【0095】ステップS240にて第2の暗／復号化処理プログラムPr1が起動されると、まず、図9に示すフローチャートのステップS1010にて、処理メニューの表示がなされる。ここで使用者が復号化処理を選択すると、ステップS1200の処理が開始される。この復号化処理を図11のフローチャートに示す。

【0096】まず、復号化対象データ名入力の実行が表示される（S1202）。次にステップS1206にてタイムアウトと判定されるまでその入力待ち（S120

4)となる。入力となされずにタイムアウトとなればステップS1206にて肯定判定されて、第2の暗/復号化処理を終了し、イニシャルプログラムに戻る。

【0097】光磁気ディスクドライブ14にセットされた光磁気ディスク内の一つのデータファイルを指定した場合(光磁気ディスク内のファイルすべてを指定しても良いし、特定のディレクトリ内のファイルをすべて指定しても良い。)、ステップS1204にて肯定判定されて、その復号化対象の暗号化データのヘッダー部より復号化対象者ID(1)、ID(2)、…および対応する暗号化された一時鍵K(1)、K(2)、…を読み出す(S1208)。

【0098】次にこの復号化対象者ID(1)、ID(2)、…内に、使用者のIDが存在するか否かが判定される(S1210)。すなわち、ICカードリーダー26にセットされているICカード30に記載されている使用者のIDが、復号化対象者として指定されているか否かが判定される。存在しなければ、現在セットされているICカード30の正当な使用者は、復号化は許可されていないので、ステップS1210にて否定判定されて、復号化は不許可であることをCRTディスプレイ16に表示して(S1220)、第2の暗/復号化処理を終了して、イニシャルプログラムに戻る。尚、複数のファイルが復号化対象として指示された場合には、ICカード30に記載されている使用者のIDが復号化対象者としてヘッダー部に指定されているファイルが一つでも存在すれば、その含まれているファイルについてだけステップS1230以降の処理を行う。また、ヘッダー部にグループのIDが指定されている場合には、ICカード30の正当な使用者がそのグループに含まれていれば、その正当な使用者はヘッダー部に指定されているとする。

【0099】ICカード30に記載された正当な使用者のIDが、復号化対象者ID(1)、ID(2)、…内に含まれている場合、例えば、ID(1)が該当すると、ステップS1210にて肯定判定されて、復号化対象ファイルのヘッダー部から読み出した暗号化された一時鍵K(1)を、ICカード30側へ送信し(S1230)、次に復号化された一時鍵の受信待ち(S1240)となる。

【0100】ICカード30側にて、ステップS590、S595およびS600を繰り返している状態で、暗号化された一時鍵K(1)を受信すると、ステップS595にて肯定判定されて、一時鍵復号化処理プログラムPr15により、暗号化された一時鍵K(1)を、バックアップRAM38に記憶している正当な使用者の暗/復号化鍵で復号化する(S630)。

【0101】次に復号化された一時鍵を情報処理装置2へ送信し(S640)、ステップS500の処理に戻る。情報処理装置2側では、復号化された一時鍵を受信したので、ステップS1240にて肯定判定されて、復号化対象データのデータ部を復号化された一時鍵で復号

化して記憶媒体に格納する(S1250)。

【0102】こうして復号化処理(S1200)が終了すると、前述したステップS1500にて、RAM8上に暗号化されていないデータ、すなわち復号化されたデータが存在する場合には、そのデータをクリアする処理が行われる。こうして、第2の暗/復号化処理が終了し、イニシャルプログラムに戻る。イニシャルプログラムでは、図6に示すステップS250の処理が行われて、RAM8上に存在している第2の暗/復号化処理プログラムをクリアし、ステップS110の処理に戻る。

【0103】このようにして、データの復号化が終了する。上述したごとく、本実施例の情報処理装置2にて起動する復号化処理用のプログラム(図9、図11)は、復号化処理に用いられていない場合には、ハードディスク装置18により暗号化された状態で記憶されている。したがって、第三者により、解析されることはなく、また解析できないので改竄もできない。

【0104】正当な使用者が復号化データを復号化する場合には、ハードディスク装置18から、正当な使用者の暗/復号化鍵にて暗号化された前記プログラムを読み出し、そのプログラムを、正当な使用者の暗/復号化鍵により復号化し、その復号化されたプログラムを起動させることにより、暗号化データを一時鍵(第2復号化鍵に該当する。すなわち一時鍵は第2暗号化鍵でも有り、第2復号化鍵でもある。)にて復号化させて復号化データ、すなわち平文データとすることができる。

【0105】しかも、暗号化データの復号化が完了した後は、その起動されたプログラムを消去する。このため、復号化処理をした後も、平文状態の復号化用のプログラムが残っていることもなく、復号化用のプログラムの安全性が確保され、結果として、データの安全性も確保される。したがって、復号化処理毎に、復号化処理用のプログラムを記憶している記憶媒体を保管場所から取り出して情報処理装置2にセットしてロードする作業をしなくても良く、効率的に復号化作業ができる。

【0106】また、復号化されたデータも作業メモリ領域上に残っている場合には、それをクリアしているので、より安全性が高い。更に、暗号化データに含まれる暗号化された一時鍵(第2復号化鍵)を、正当な使用者の暗/復号化鍵にて復号化する。

【0107】このようにすることにより、暗号化データを復号化するための一時鍵(第2復号化鍵)が得られ、正当な使用者のみが適切に暗号化データを復号化して平文データを得ることができる。また、本実施例では、本体装置としての情報処理装置2と、この情報処理装置2とは別体に構成され情報処理装置2に対して信号的に任意に接続したり切断したりすることが可能な付属装置としてのICカード30とに別れて構成され、情報処理装置2が、プログラム暗号化記憶処理、プログラム読出処理、プログラム起動処理、およびプログラム消去処理の

各プログラムを備え、ICカード30が、正当な使用者の暗/復号化鍵を記憶するとともに、プログラム復号化処理および鍵復号化処理のプログラムを備える構成とされている。

【0108】このように構成されているため、ICカード30側には、正当な使用者の暗/復号化鍵、プログラム復号化処理および鍵復号化処理のプログラムが存在するため、その正当な使用者に対応する暗/復号化鍵、プログラム復号化処理のプログラムおよび鍵復号化処理のプログラムの安全性が確保され、データの安全性が一層確保される。

【0109】次に、ハードディスク装置18に記憶されている、暗号化された第2の暗復号化処理プログラムの変更処理について説明する。使用者は、まず、情報処理装置2の電源オンさせた後、受け取った光磁気ディスクを光磁気ディスクドライブ14にセットし、自己のICカード30をICカードリーダー26にセットする。

【0110】情報処理装置2では、イニシャルプログラムが起動される。この場合の処理は、ステップS100からステップS240までは、データ暗号化あるいは復号化の際に説明した通りである。ICカード30においても同様である。勿論、使用者が異なれば、ICカード30も異なることから、ステップS170にて受信するIDも異なり、ステップS210にてICカード30へ送信される暗号化された第2の暗/復号化処理プログラムも異なる。

【0111】例えば、使用者のIDがIDcであれば、暗号化された第2の暗/復号化処理プログラムPr3が対応していることから、暗号化された第2の暗/復号化処理プログラムPr3が、ICカード30へ送信され、その結果、ステップS240により起動されるプログラムは、第2の暗/復号化処理プログラムPr3が実行される。ステップS240にて第2の暗/復号化処理プログラムPr3が起動されると、まず、図9に示すフローチャートのステップS1010にて、処理メニューの表示がなされる。

【0112】ここで使用者がプログラム変更処理を選択すると、ステップS1300の処理が開始される。プログラム変更処理を図12のフローチャートに示す。まず、第2の暗/復号化処理プログラムの編集処理がなされる(S1302)。例えば、16進数にて表現されている第2の暗/復号化処理プログラムを逆アセンブルして、アセンブリ言語にて表現し、キーボード12による編集可能とする。編集が終了すれば、編集後の内容がアセンブルされ、実行可能なプログラムに変換される。

【0113】尚、この編集処理では、単に既に変更されている他のプログラムと置き換える処理も含まれる。したがって、他の装置で作成したプログラムを新たに、第2の暗/復号化処理プログラムとして取り込むことができる。また、この編集処理では、単にプログラム中に設

定されている数値や文字列等のデータの変更も含まれる。

【0114】次に、編集後の第2の暗/復号化処理プログラムをICカード30側へ送信し(S1304)、暗号化された第2の暗/復号化処理プログラムの受信待ち(S1306)となる。ICカード30側にて、ステップS590、S595およびS600を繰り返している状態で、暗号化していない第2の暗/復号化処理プログラムを受信すると、ステップS600にて肯定判定されて、プログラム暗号化処理プログラムPr12により、ICカード30の正当な使用者の暗/復号化鍵により第2の暗/復号化処理プログラムを暗号化する(S650)。

【0115】次に、この暗号化された第2の暗/復号化処理プログラムを情報処理装置2へ送信し(S660)、ステップS500の処理に戻る。情報処理装置2側では、暗号化された第2の暗/復号化処理プログラムを受信したので、ステップS1306にて肯定判定され、次に暗号化された第2の暗/復号化処理プログラムをハードディスク装置18に収納し、そのディスクアドレスを、使用者ID-プログラムアドレステーブルの内、IDcと対応させたプログラムアドレスPr3に記入する(S1308)。

【0116】こうして、プログラム変更処理を終了する。以後、ステップS1500の処理を行って、イニシャルプログラムに戻る。イニシャルプログラムでは、ステップS250の処理が行われて、RAM8上に存在している第2の暗/復号化処理プログラムをクリアし、ステップS110の処理に戻る。

【0117】上述したごとく、本実施例の情報処理装置2にて起動するプログラム変更処理(図9、図12)は、正当な使用者により、その使用者専用の暗号化された第2の暗/復号化処理プログラムの内容を変更できるので、その使用者毎に異なるアルゴリズムや異なる設定値(プログラム中のデータを変更した場合)にて暗/復号化することが可能となる。

【0118】したがって、使用者毎にプログラムを変更しておけば、一人の暗/復号化アルゴリズムが第三者に解析された場合にも、同時に全員のプログラムまで解析されることはない。また、解析された場合には、プログラム変更処理により、正当な使用者がプログラムを変更することにより、以後の情報については安全性が確保できる。

【0119】また本実施例において、入力操作が行われない場合は、タイムアウト処理(S1106、S1206)により第2の暗/復号化処理プログラムを終了し、ステップS250の処理が行われて、RAM8上に存在している第2の暗/復号化処理プログラムをクリアしているので、使用者が処理の途中で情報処理装置2を離れても、第三者による解析や改竄を防止できる。ステッ

プS1302にても編集の途中で操作が行われなくなれば、第2の暗/復号化処理プログラムを終了しても良い。

【0120】また、情報処理装置2側では、データ量の大きい暗号化対象のデータの暗号化あるいは復号化処理を行い、ICカード30側では、データ量の小さいプログラムや一時鍵の暗号化あるいは復号化処理を行うので、全体の処理としては高速に行うことができる。また、ICカード30としては小さくて安価な構成とすることができる。

【0121】また、図13に示したごとく、復号化を許可する者の数に対応して暗号化されるのは一時鍵のみであり、実際の暗号化データは一つのみ存在することから、保管、運搬あるいは通信するデータ量は、復号化を許可する者の数が多くても、膨大なデータ量とはならず、メモリや記憶媒体あるいは通信時間が節約できる。

【0122】本実施例において、ハードディスク装置18がプログラム暗号化記憶手段に該当し、ステップS210がプログラム読出手段としての処理に該当し、ステップS570がプログラム復号化手段としての処理に該当し、ステップS240がプログラム起動手段としての処理に該当し、ステップS250がプログラム消去手段としての処理に該当し、ステップS610が鍵暗号化手段としての処理に該当し、ステップS1160が鍵付加手段としての処理に該当し、ステップS630が鍵復号化手段としての処理に該当する。

【0123】〔その他〕上述した実施例は、データを暗号化したり、あるいは暗号化したデータを復号化して平文データに戻す情報秘匿処理システムであったが、更に、情報処理装置2が制御装置およびモデムを備えることにより、正当な使用者が前記実施例のごとくデータを暗号化して通信回線を介して相手方に送信し、また相手方が通信回線を介して送信して来た暗号化データを、前記実施例のごとく正当な使用者（復号化対象者）が復号化して平文データとして得る情報秘匿通信システムとして構成しても良い。

【0124】更に、この情報秘匿通信システムに、原稿の画像読取装置および画像の記録装置を備えることにより、ファクシミリ装置として構成し、その原稿の画像データを、前記実施例のごとく、暗号化あるいは復号化の対象としても良い。前記実施例では、正当な使用者や復号化対象者をIDで指定していたが、IDでなくても対象者名でも良いし、IDと対象者名との両方でも良い。

【0125】前記実施例では、ICカード30に記憶されている正当な使用者の暗/復号化鍵は、暗号化にも復号化にも用いられたが、暗号化時は公開鍵を用い、復号化時には秘密鍵を用いても良い。したがって、正当な使用者がデータの復号化を許可する相手方暗号化鍵K1、K2、…、Knは公開鍵であっても良い。

【0126】またICカード30のバックアップRAM

38には、復号化を許可する相手方のID1、ID2、…とそれに対応した暗号化鍵K1、K2、…とが記憶されていたが、直接、このようなIDと暗号化鍵Kとを記憶するのではなく、次のようにしても良い。

【0127】すなわち、バックアップRAM38に秘密のアルゴリズムを内蔵し、復号化を許可する相手方のIDを入力すると、そのアルゴリズムにしたがって演算処理にて対応する暗号化鍵Kを生成する構成としても良い。この構成にすると複数の暗号化鍵を記憶しなくても、一つのアルゴリズムのみで、多数のIDから暗号化鍵を得ることができるので、復号化を許可する者が多い場合には、メモリの節約となる。

【0128】このIDから演算処理で鍵を生成する構成を、ICカード30の正当な使用者の暗/復号化鍵に対しても適用して、正当な使用者のIDから暗/復号化鍵を生成するようにしても良い。また、ICカード30は、バックアップRAM38にプログラムや各鍵等を保管しているので、外装に連動して外装開放時にオフとなるスイッチをバックアップ電源とバックアップRAM38との間に用いれば、外装を開けるとプログラムや鍵等が消去されることから、安全上、より好ましい。また、バックアップRAM38の代りに、EEPROMにプログラムや鍵等を記憶しても良い。この場合は、外装と連動して外装開放時にオンとなるスイッチを電源とEEPROMとの間に設ければ、外装を開けると電流が流れてプログラムや鍵等が消去される。

【0129】前記実施例において、イニシャルプログラムはハードディスク装置18でなく、ROM6に格納されていても良い。

【図面の簡単な説明】

【図1】 本発明一実施例を構成する情報処理装置のブロック図である。

【図2】 本発明一実施例を構成するICカードのブロック図である。

【図3】 情報処理装置におけるプログラムおよびデータの記憶配置説明図である。

【図4】 ICカードにおけるプログラムおよびデータの記憶配置説明図である。

【図5】 情報処理装置におけるイニシャルプログラムのフローチャートである。

【図6】 情報処理装置におけるイニシャルプログラムのフローチャートである。

【図7】 ICカード側処理のフローチャートである。

【図8】 ICカード側処理のフローチャートである。

【図9】 第2の暗/復号化処理のフローチャートである。

【図10】 第2の暗/復号化処理の内の暗号化処理のフローチャートである。

【図11】 第2の暗/復号化処理の内の復号化処理のフローチャートである。

【図12】 第2の暗/復号化処理の内のプログラム変更処理のフローチャートである。

【図13】 暗号化データの構成説明図である。

【符号の説明】

2…情報処理装置 4…CPU 6…ROM
8…RAM
10…バックアップRAM 12…キーボード
14…光磁気ディスクドライブ 16…CRTディスプレイ

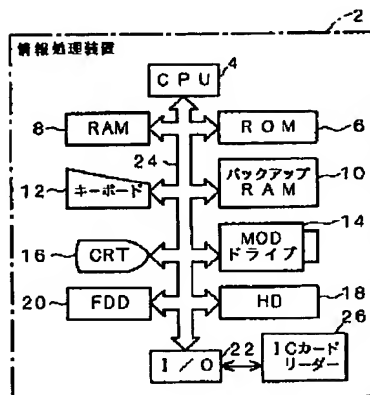
18…ハードディスク装置 20…フロッピーディスクドライブ

22…I/O 24…バス 26…ICカードリーダー

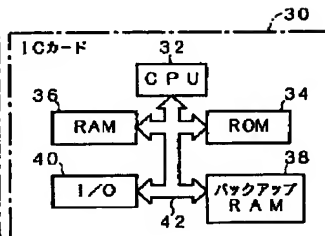
30…ICカード 32…CPU 34…ROM
36…RAM

38…バックアップRAM 40…I/O 42…バス

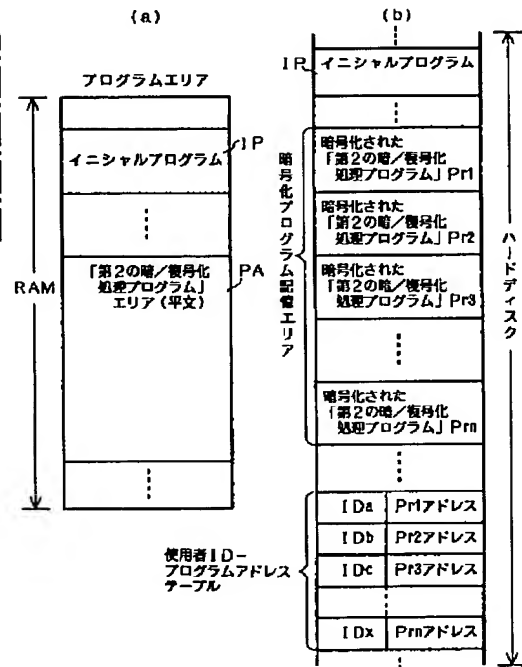
【図1】



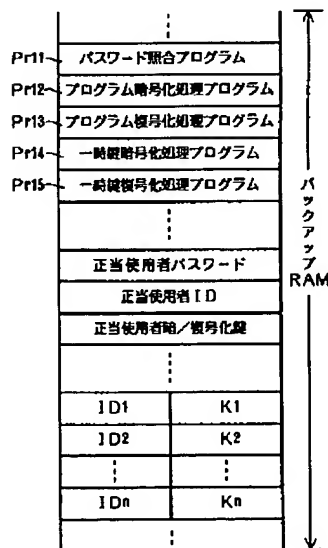
【図2】



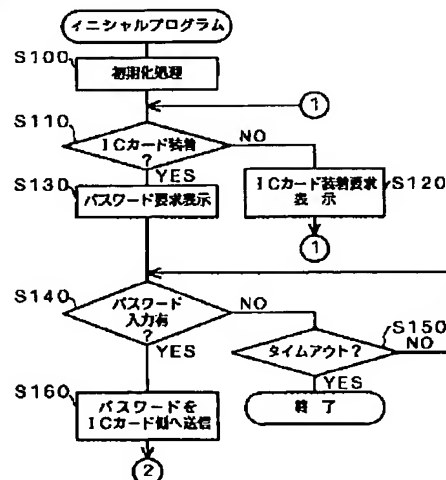
【図3】



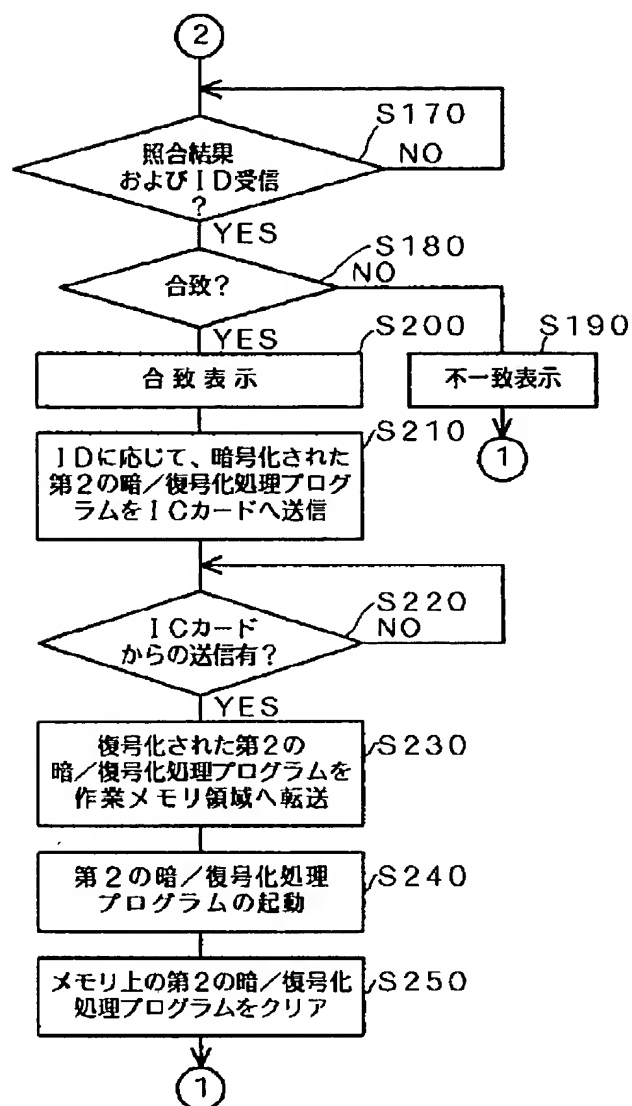
【図4】



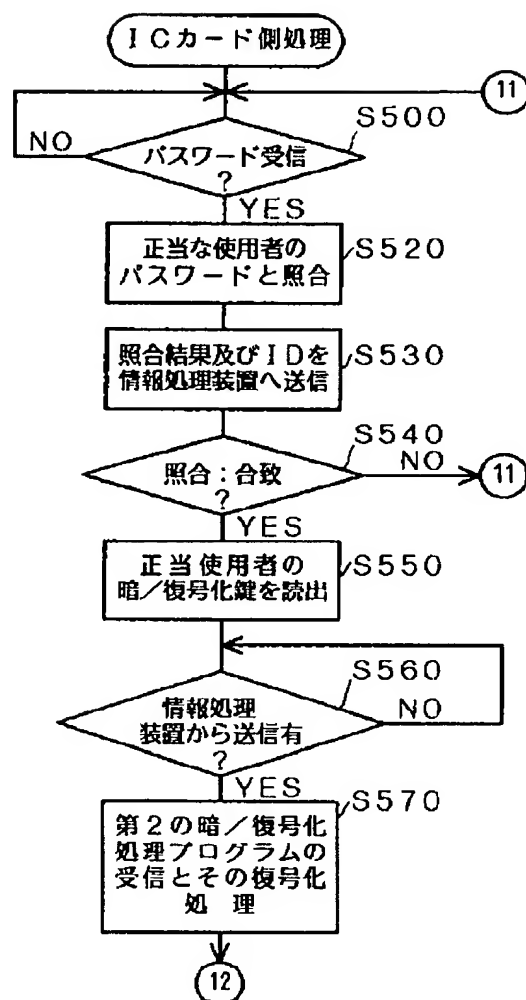
【図5】



【図6】



【図7】

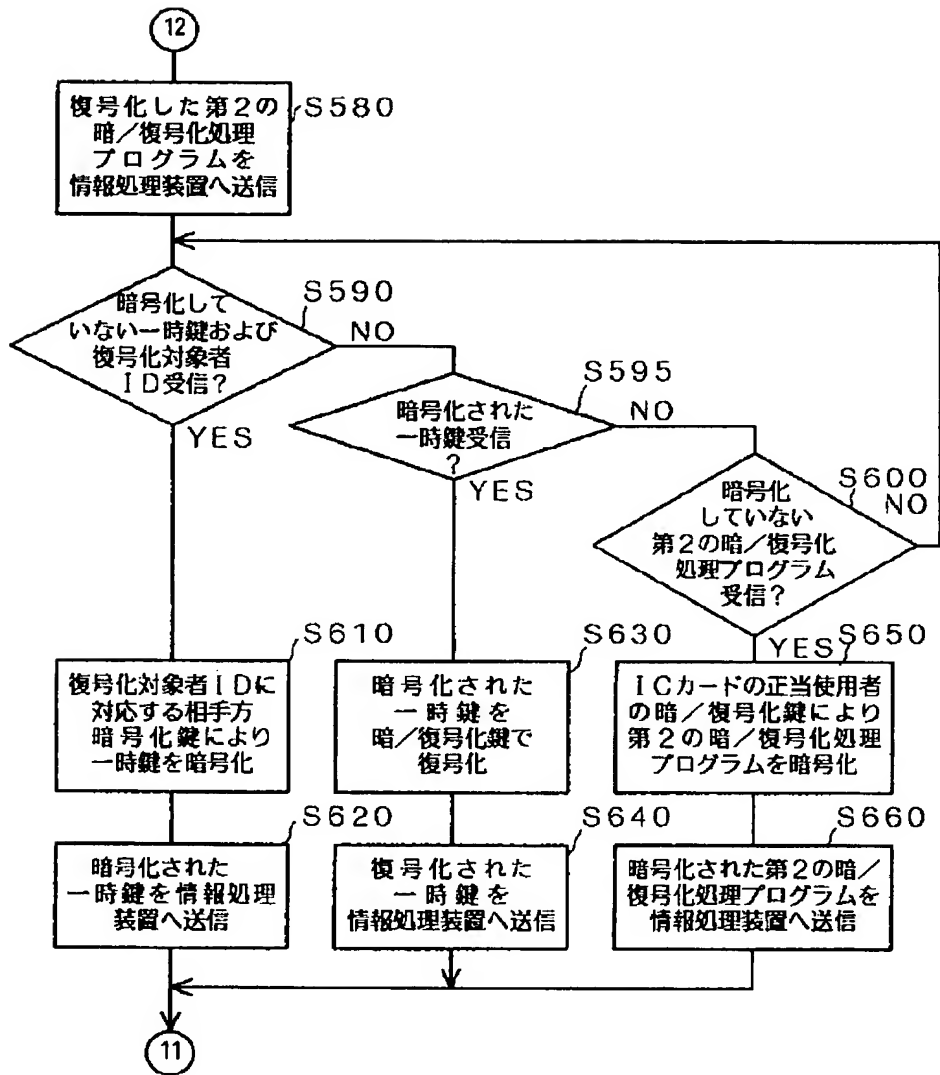


【図13】

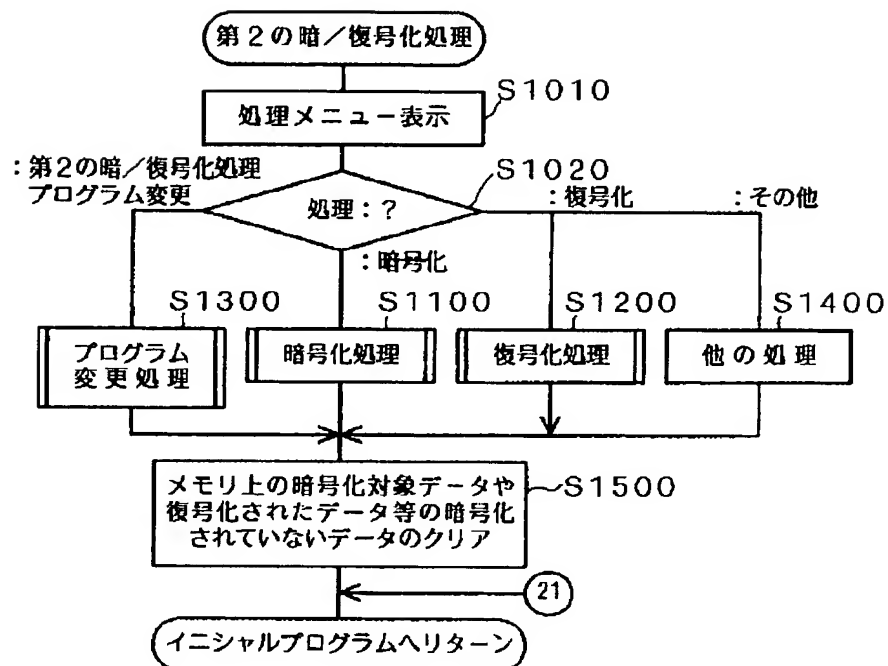
ヘッダー部	復号化対象者1のID(1)	ID(1)に対応した暗号化一時鍵 K(1)
	復号化対象者2のID(2)	ID(2)に対応した暗号化一時鍵 K(2)

	復号化対象者nのID(n)	ID(n)に対応した暗号化一時鍵 K(n)
データ部	暗号化データ	

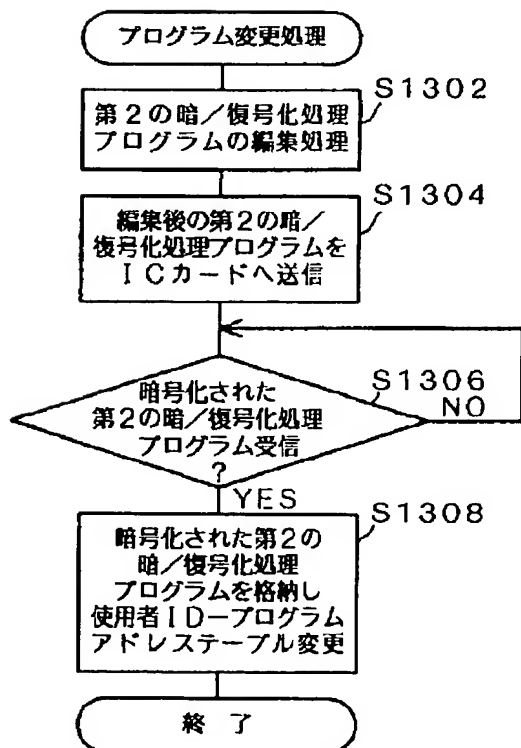
【図8】



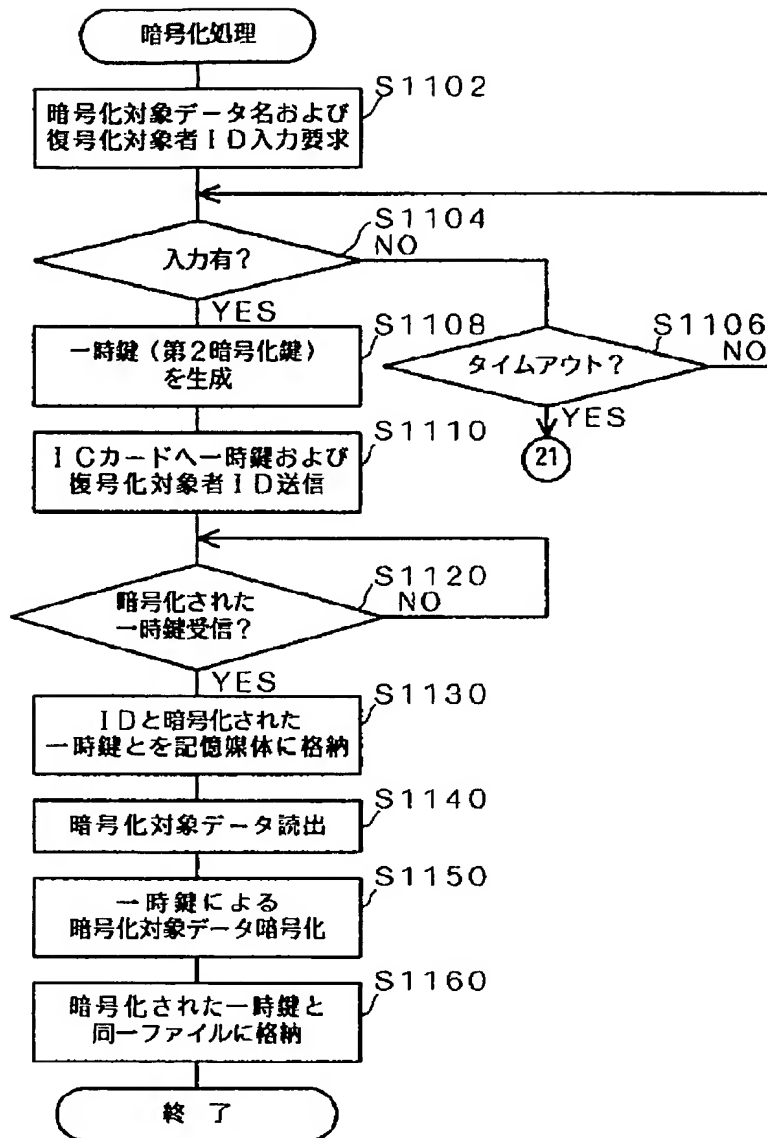
【図9】



【図12】



【図10】



【図11】

